REMARKS / DISCUSSION OF ISSUES

This submission is in response to the Office Action dated January 7, 2008 (the "Office Action"). Claims 1– 6 are pending in the application. Applicants have amended claim 1 without prejudice or disclaimer.

Rejections under 35 U.S.C. §103(a)

A. Claims 1-3, 8-10 are allowable

The Office has rejected claims 1–6 under 35 U.S.C. §103(a) as being unpatentable over "Intrusion Detection Using Static Analysis" (hereinafter "Wagner") in view of "Static Analysis" (hereinafter "Webb") and further in view of "Splint Manual" (hereinafter "Splint"). Applicants respectfully traverse the rejections.

Independent Claim 1 has been amended herein to better define Applicants' invention over the combined references. Claim 1 now recites limitations and/or features which are not disclosed by Wagner, Webb and Splint Manual, alone and in combination.

In the Final Office Action, Splint is cited as a static analysis tool capable of examining all the parameters and return values of functions and compare them to establish that no mismatch exists. The Office refers Applicants to pages 19-24, "4 Types"). Claim 1 has been amended to recite "*checking a script to determine whether a series of methods constructing a malicious code pattern exist and whether parameters and return values associated between the methods that satisfy a generated matching rule match each other*" (Emphasis Added). It is respectfully submitted that checking only those parameters and return values associated between methods that satisfy a generated matching rule is different from checking whether all parameters and return values associated between the methods match each other.

In the Final Office Action, the Examiner maintains his rejection of Claim 1, citing Wagner for allegedly teaching the checking step of claim 1. As recited in Claim 1, the checking step further comprises the steps of (1) modeling malicious behavior to include unit behaviors comprised of sub-unit behaviors and method calls, (2) converting each identified unit behavior and method call sentence into a matching rule and (3) generating at least one relation rule for defining a relation between rule variables used in the sentences satisfying the matching rule. The Office directs the Applicants' attention to section 4.3, "The abstract stack model", and particularly pages 160-161, "The context-free model" in support of the rejection. Upon close review of Wagner, Applicants respectfully submit that Wagner does not teach the checking step of claim 1. Both the "abstract stack model" and the "context-free model" of Wagner are based on expected application behavior built statically from program source code. At run-time, a suspect program is monitored and checks are made to determine whether the system call traces for the suspect program are in compliance with the model. See Figure 2 of Wagner as an illustration of the abstract stack model. Applicants submit that "modeling malicious behavior to include unit behaviors comprised of sub-unit behaviors and method calls, converting each identified unit behavior and method call sentence into a matching rule and generating at least one relation rule for defining a relation between rule variables used in the sentences satisfying the matching rule," as recited in claim 1, is dynamic in the sense that it is **not** based on expected application behavior built statically from program source code.

In the Final Office Action, Webb is cited for allegedly teaching the step of "*generating instances of the matching rule comprising the steps of i) searching for code patterns matched within the matching rules from a relevant script code to be detected, ii) extracting parameters of functions used in the searched code patterns, and iii) storing the extracted parameters of functions used in the searched code patterns.*" The Office asserts that while Wagner does not disclose this step, Webb remedies this deficiency by allegedly teaching the ability to statically analyze local variables, data structure, and all other data

flow in a script so as to determine if the script is non-hazardous has been long since known in the art, and has even been realized in pre-existing products. Applicants submit that the rejection does not address the particulars of the claim recitation and is broad brush statement with little to no applicability to the claim language. Specifically, the applicability of the Office's comments regarding the ability to statically analyze local variables, data structure, and all other data flow in a script so as to determine if the script is non-hazardous is not remotely germane to the step of "*generating instances of the matching rule comprising the steps of i) searching for code patterns matched within the matching rules from a relevant script code to be detected, ii) extracting parameters of functions used in the searched code patterns, and iii) storing the extracted parameters of functions used in the searched code patterns.*" The only explanation offered by the Office is incorporation of the ability to statically analyze local variables, data structure, and all other data flow in a script so as to determine if the script is non-hazardous would negate the need to make simplistic assumptions regarding the behavior of scripts to be tested. Applicants respectfully assert that this reasoning does even remotely not address the claim language recited above in any meaningful way.

Claim 1 has been further amended to better define Applicant's invention over the combined references. In particular, Claim 1 as amended now recites:

> c) generating at least one relation rule for defining a relation between rule variables used in the sentences satisfying the matching rule **by analyzing a relation between the rule identifiers used in the sentences patterns satisfying the matching rule;**

and

> e) generating instances of the relation rule by searching for instances of the matching rule satisfying the relation rule from the set of the generated instances of the matching rule **through a relation analysis process by continuously checking whether previously generated instances of the relation rule associated with a currently generated instance of the relation rule are satisfied.**

Claims 2-6 depend from claim 1, which Applicants have shown to be allowable. Thus, claims 2-6 are allowable, at least by virtue of their dependency from claim 1.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the cited portions of the cited references as applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allow ability of each of the pending claims.

Any changes to the claims in this response, which have not been specifically noted to overcome a rejection based upon the prior art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims presently pending in the application, namely, Claims 1–6 are believed to be in condition for allowance and patentably distinguishable over the art of record. Please contact the undersigned attorney should there be any questions. A petition for an automatic three-month extension of time for response under 37 C.F.R.§1.136(a) is enclosed in triplicate together with the requisite petition fee, RCE transmittal and filing fee.

Early favorable action is earnestly solicited.

Respectfully submitted,

George M. Kaplan
Reg. No. 28,375
Attorney for Applicant(s)

DILWORTH & BARRESE, LLP
333 Earle Ovington Blvd.
Uniondale, New York 11553
Phone: 516-228-8484
Facsimile: 516-228-8516